(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 March 2002 (28.03.2002)

PCT

(10) International Publication Number
WO 02/25402 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US01/29336

(22) International Filing Date:
19 September 2001 (19.09.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/666,114 20 September 2000 (20.09.2000) US

(71) Applicant *(for all designated States except US)*: **BBNT SOLUTIONS LLC** [US/US]; 10 Moulton Street, Cambridge, MA 02138 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **DONAGHEY, Robert, J.** [/US]; 40 Oak Street, Lexington, MA 02421 (US).

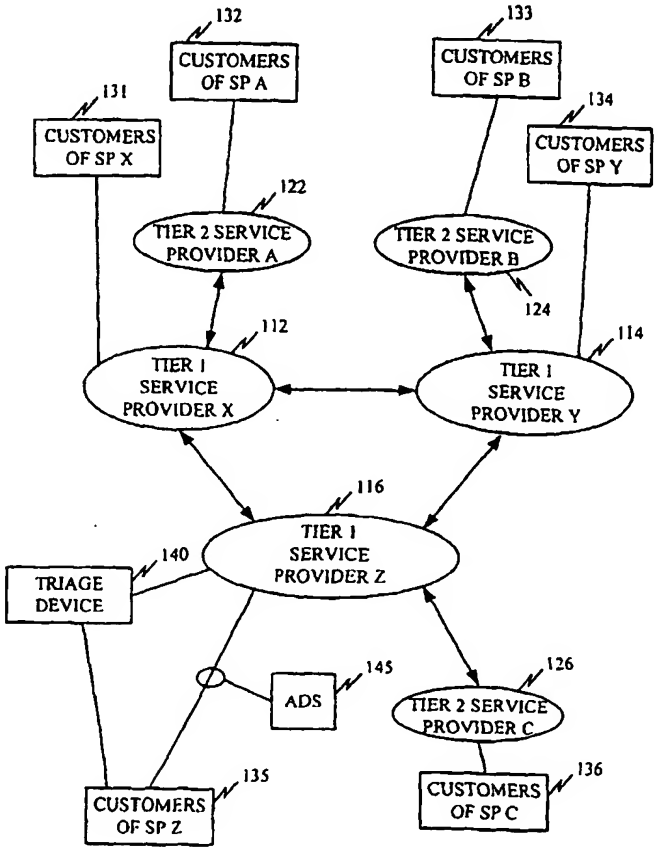
(74) Agent: **SUCHYTA, Leonard, Charles**; c/o Christian R. Anderson, Verizon Services Group, 600 Hidden Ridge Drive, Mailcode HQE03H01, Irving, TX 75038 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: SYSTEMS AND METHODS THAT PROTECT NETWORKS AND DEVICES AGAINST DENIAL OF SERVICE ATTACKS



(57) Abstract: A system protects communicaton networks and devices against denial of service (DoS) attacks. A service provider (116) receives a signal indicating that a DoS attack has been detected, receives one or more packets intended for a victim device (420), and transmits the one or more packets to a triage device (140). The triage device determines whether each of the one or more packets is part of the DoS attack and forwards only packets that are deemed unrelated to the DoS attack to the victim device (420).

WO 02/25402 A2

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Published:

— *without international search report and to be republished upon receipt of that report*

SYSTEMS AND METHODS THAT PROTECT NETWORKS AND DEVICES AGAINST DENIAL OF SERVICE ATTACKS

FIELD OF THE INVENTION

The present invention relates generally to networks and, more particularly, to systems and methods that protect communication networks and devices from denial of service attacks.

BACKGROUND OF THE INVENTION

Denial of Service (DoS) attacks represent a major threat to the continuous operations of network devices. In a typical Distributed DoS (DDoS) attack, traffic emanates from a wide range of compromised systems, and packets from these systems are directed at one or more target hosts, e.g., web servers. When a DoS attack occurs across an Internet Service Provider's (ISP's) network, the transmission network may become so congested that the ISP can no longer provide adequate service. Examples of DoS attacks include smurf attacks, SYN flood attacks, and Ping of Death attacks. All of these may be effected as distributed DoS attacks, where many compromised network devices become the unwitting source of DoS traffic.

A smurf attack is an assault on a network that floods the network with excessive messages in order to impede normal traffic. An attacking device sends ping requests to a broadcast address on the target network. The attacking device sets the return address to the victim's address. The broadcast address can generate hundreds of response messages from unwitting network devices that eventually overload the target network.

A SYN flood attack is an assault on a network that prevents a Transmission Control Protocol/Internet Protocol (TCP/IP) server from servicing other users. An attacking device sends a counterfeit source address to the server so that a final

acknowledgment to the server's SYNchronize-ACKnowledge (SNY-ACK) response in the handshaking sequence is not sent. As a result, the server continues to execute the handshaking sequence until the server either overloads or crashes.

A Ping of Death attack is an assault on a target computer. An attacking device causes the target computer to crash by sending a packet having an invalid packet size value in the packet's header.

To date, major work on combating DoS attacks has focused on router and firewall-based packet filtering mechanisms designed to reject traffic based on simple filtering rules. Ingress packet filtering by ISPs makes tracking attack sources easier, by limiting the range of spoofed source addresses available to DoS traffic generators, but it does not prevent such traffic from reaching targets. Since DoS traffic streams often originate from outside a target's ISP, and because it is currently infeasible to filter traffic at border gateway protocol (BGP) peering points, ingress filtering relies on all other ISPs to provide protection, a bad strategy in the global Internet environment.

With the proliferation of freely available DoS attack software, DoS attacks will become more sophisticated and more frequent and, therefore, produce more far-reaching consequences in the future. Simple filtering, based on examination of IP and TCP layer headers, will become less and less effective against more sophisticated attacks. Even traffic characterization technologies, such as Multi-Protocol Layer Switching (MPLS), that employ high speed header analysis facilities will become inappropriate for filtering DoS traffic, as the rapid reconfiguration required to respond to attacks would impose a serious burden on the backbone traffic engineering system, which is optimized for packet forwarding.

Current attempts to prevent DoS attacks involve an ISP's network operations center (NOC) manually attempting to intervene in the attack. If the DoS attack is successful, the NOC may not be able to "break into" the network connection to thwart the attack. As a result, the NOC may need to spend many hours trying to filter the attacker's data out of their network, while at the same time calming their customers.

Since a successful DoS attack causes the customer's local network, firewall, and possibly web server to become unstable and/or unusable, those customers who rely on electronic commerce are particularly affected by DoS attacks. Unfortunately, the most advanced intrusion detection systems look for specific signatures of attacks in a data flow and then send a message to an operator for manual intervention. By the time the operator attempts to intervene, however, damage from the DoS attack may have already occurred.

Therefore, there exists a need for systems and methods that better protect against DoS attacks.

SUMMARY OF THE INVENTION

Systems and methods consistent with the present invention address this and other needs by providing a process that protects communication networks and devices against denial of service attacks.

In accordance with the purpose of the invention as embodied and broadly described herein, a system protects against DoS attacks. The system includes a service provider and a triage device. The service provider receives a signal indicating detection of a DoS attack, receives one or more packets intended for a victim device, and transmits the one or more packets to the triage device. The triage device determines, for each received packet, whether the packet is part of a

DoS attack and forwards any packets that are unrelated to the DoS attack to the victim device.

In another implementation consistent with the present invention, a method protects against DoS attacks. The method includes detecting the occurrence of a DoS attack, determining a target of the DoS attack, intercepting packets destined for the target, and preventing packets that are related to the DoS attack from reaching the target.

In still another implementation consistent with the present invention, a device for protecting against DoS attacks is provided. The device includes a memory and a processor that receives, once a DoS attack has been detected, packets from a service provider, determines, for each packet addressed to the intended target, whether a packet is part of the DoS attack, forwards a packet determined not to be part of the DoS attack to a target device, and discards and/or proxies a reply to a packet determined to be part of the DoS attack.

In a further implementation consistent with the present invention, a method that protects against DoS attacks is provided. The method includes passively recording, via an attack detection sensor, packets transmitted in a network, detecting an occurrence of a DoS attack, transferring, in response to the detecting, packets for a target of the DoS attack from a service provider to a triage device, retrieving recently recorded packets from the attack detection sensor, determining, for each transferred packet, whether the packet is part of the DoS attack, forwarding a packet determined not to be part of the DoS attack to the target, and discarding or proxying a reply to a packet determined to be part of the DoS attack.

In yet another implementation consistent with the present invention, a passive DoS attack sensor is provided. The DoS attack sensor includes a memory

that stores instructions and information relating to packets transferred in a network. The DoS attack sensor also includes a processor that monitors the packets, stores the information in the memory, detects a DoS signature in one or more of the packets, sends a signal to a service provider in response to the detecting, and transfers the information in the memory for use in determining a history of the one or more packets.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate an embodiment of the invention and, together with the description, explain the invention. In the drawings,

FIG. 1 illustrates an exemplary network in which systems and methods, consistent with the present invention, that protect against denial of service attacks may be implemented;

FIG. 2 illustrates an exemplary triage device or attack detection sensor device configuration consistent with the present invention;

FIG. 3 illustrates an exemplary database that may be associated with the triage device or attack detection sensor device of FIG. 2;

FIG. 4 illustrates an exemplary denial of service attack scenario;

FIG. 5 illustrates exemplary processing of an attack detection sensor consistent with the present invention; and

FIGS. 6A and 6B illustrate an exemplary process for protecting communication networks and devices against denial of service attacks in an implementation consistent with the present invention.

DETAILED DESCRIPTION

The following detailed description of the invention refers to the accompanying drawings. The same reference numbers in different drawings

identify the same or similar elements. Also, the following detailed description does not limit the invention. Instead, the scope of the invention is defined by the appended claims.

Systems and methods consistent with the present invention protect communication networks and devices against denial of service attacks. Upon detection of a DoS attack, a service provider redirects traffic away from a targeted host (or hosts) and toward a triage device, that may use a combination of packet destruction, proxying for the target, other filtering mechanisms and prioritized packet forwarding to protect intended targets from attack. The triage device diverts the brunt of the attack from the targets, allowing them to continue to operate during a DoS attack. Even DoS attacks that might overwhelm the access link capacity of a target can be handled by the triage device, since a service provider can provision very high capacity access links for this service. Network devices can be configured to automatically detect DoS attacks and trigger the invocation of the triage device, and attacked hosts can request the invocation of the triage device through any available communication channels.

EXEMPLARY NETWORK

FIG. 1 illustrates an exemplary network 100 in which systems and methods, consistent with the present invention, that protect against denial of service attacks may be implemented. In FIG. 1, network 100 includes multiple tier one service providers (SPs) 112-116, tier two service providers 122-126, customers 131-136, a triage device 140, and an attack detection sensor (ADS) 145.

The tier one SPs 112-116 may include, for example, large national ISPs. The tier one SPs exchange traffic with each other directly. This is known as peering. Every tier one SP peers with every other tier one SP.

The tier two SPs 122-126 may include, for example, regional ISPs or

smaller SPs that rely on a tier one SP to provide transit service. The tier two SPs generally connect to one or more tier one SP.

The customers 131-136 may include one or more host devices (not shown) that connect to a corresponding tier one or tier two SP 112-126 via a wired, wireless, or optical connection. The host devices may include, for example, a server, personal computer, or the like. The host devices may be directly connected to a SP 112-126 or may be connected to a SP 112-126 through one or more local networks (not shown).

The triage device 140 may include, according to an exemplary implementation, a high-end computer, a server or collection of servers, or the like, capable of protecting one or more network devices in response to a DoS attack. The triage device 140 may be connected to, or implemented within, a SP 112-126 or another network device. Connection of the triage device 140 to a SP 112-126 or network device should be of such a capacity so as not to be overwhelmed by the large amount of traffic commonly associated with DoS attacks. As illustrated in FIG. 1, the triage device 140 connects to a SP or network device in such a way as to be out of the regular flow of network traffic. Network traffic may, as will be described in more detail below, be routed through the triage device 140 in those situations where a DoS attack has been detected.

The attack detection sensor device 145 may include, according to an exemplary implementation, a personal computer or the like, capable of passively monitoring traffic and detecting the presence of a DoS attack. The attack detection sensor device 145 may be connected to, or implemented within, a SP 112-126 or another network device.

The number of components illustrated in FIG. 1 is provided for simplicity. In practice, a typical network 100 may include a larger or smaller number of SPs

112-126, customers 131-136, triage devices 140, and attack detection sensor devices 145.

EXEMPLARY TRIAGE DEVICE/ADS DEVICE CONFIGURATION

FIG. 2 illustrates an exemplary triage device 140 or attack detection sensor device 145 configuration consistent with the present invention. The exemplary triage/ADS device 140/145 includes a bus 202, a processor 204, a main memory 206, a read only memory (ROM) 208, a storage device 210, an optional input device 212, an optional output device 214, and a communication interface 216. The bus 202 permits communication among the components of the triage/ADS device 140/145.

The processor 204 may include any type of conventional processor or microprocessor that interprets and executes instructions. The main memory 206 may include a random access memory (RAM) or another type of dynamic storage device that stores information and instructions for execution by the processor 204. Main memory 206 may also be used to store temporary variables or other intermediate information during execution of instructions by processor 204.

ROM 208 may include a conventional ROM device and/or another type of static storage device that stores static information and instructions for processor 204. The storage device 210 may include a magnetic disk or optical disk and its corresponding drive and/or some other type of magnetic or optical recording medium and its corresponding drive for storing information and/or instructions.

The input device 212 (if any) may include any conventional mechanism that permits an operator to input information to the triage/ADS device 140/145, such as a keyboard, a mouse, a microphone, a pen, voice recognition and/or biometric mechanisms, etc. The output device 214 (if any) may include any

conventional mechanism that outputs information to the operator, including a display, a printer, a pair of speakers, etc.

The communication interface 216 may include any transceiver-like mechanism that enables the triage/ADS device 140/145 to communicate with other devices and/or systems, such as SPs 112-126 or customers 131-136. For example, the communication interface 216 may include a modem or an Ethernet interface to a network. Alternatively, communication interface 216 may include other mechanisms for communicating via a data network.

The triage/ADS device 140/145 protects against denial of service attacks in response to processor 204 executing sequences of instructions contained in a computer-readable medium, such as memory 206. It should be understood that a computer-readable medium may include one or more memory devices and/or carrier waves. The instructions may be read into memory 206 from another computer-readable medium, such as a storage device 210, or from a separate device via communication interface 216. Execution of the sequences of instructions contained in memory 206 causes processor 204 to perform the process steps that will be described hereafter. In alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the present invention. Thus, the present invention is not limited to any specific combination of hardware circuitry and software.

An ADS device 145, consistent with the present invention, logs all recent traffic (e.g., using a circular buffer) on a continuous basis in order to provide limited audit trail data for later analysis and prosecution. The attack detection sensor device 145 may log this information in an associated database. The database may be stored at the attack detection sensor device 145 (e.g., in main memory 206) or externally from attack detection sensor device 145.

A triage device 140, consistent with the present invention, logs all traffic during an attack in order to provide extensive forensics data for later analysis and prosecution. The triage device 140 may log this information in an associated database. The database may be stored at the triage device 140 (e.g., in main memory 206) or externally from triage device 140.

FIG. 3 illustrates an exemplary database 300, consistent with the present invention, that may be associated with triage/ADS device 140/145. While only one database is described below, it will be appreciated that database 300 may consist of multiple databases stored locally at each triage device 140 and ADS device 145 or stored at different locations throughout the network 100.

As illustrated, database 300 includes a group of entries 305. Each entry 305 includes information stored in one or more of the following exemplary fields: a source address field 310, a target address field 320, a date field 330, a time field 340, and a log entry field 350. Database 300 may contain additional fields that would aid the triage/ADS device 140/145 in searching, sorting, and/or providing information for analyzing a DoS attack.

The source address field 310 stores an address from a packet of information determined to be part of a DoS attack that identifies the network device from where the packet was sent, although this information will typically not be reliable. The target address field 320 stores an address of the target network device to which the packet of information was sent. The date field 330 stores the date on which the packet was received. The time field 340 stores the time at which the packet was received. The log entry field 350 stores additional information relating to the DoS attack that may aid in determining the nature of a DoS attack. This information may be automatically entered by the triage device 140 or may be entered by an operator.

EXEMPLARY ATTACK SCENARIO

FIG. 4 illustrates an exemplary scenario 400 in which a group of adversarial network devices 410 participate in a DDoS attack on a host device 420. In a typical DoS attack, traffic emanates from a wide range of compromised systems, and packets from these systems are directed at one or more target hosts, e.g., web servers. The number of adversarial devices 410 illustrated in FIG. 4 is provided for simplicity. A typical attack scenario 400 would generally include a larger number of adversarial devices 410.

As illustrated, a number of adversarial devices 410 transmit packets of information through their associated SPs 412 in an attempt to attack host device 420. A passive attack detection sensor 145 detects a DDoS attack on host 420 and notifies the SP 412 which invokes the triage service 140. In an implementation consistent with the present invention, the attack detection sensor 145 maintains a limited audit trail (e.g., circular buffer) on a continuous basis. The attack detection sensor 145 may send its buffer contents to the triage device's database 300 to assist in characterizing the early or precursor phases of an attack. The attack detection sensor 145 may be implemented as a purely passive system so that it does not impose any delays on traffic, nor would its failure affect normal operation of the target systems.

In an alternative implementation, host 420 (or some other network device) may detect the DoS attack and notify service provider 116 that an attack is underway. The host 420 may notify the service provider 116 via any conventional technique, such as a telephone call, e-mail, facsimile, etc.

Once an attack has been detected, routing within the target's SP 116 may be altered to divert all traffic for the target host 420 to the triage device 140. For every packet directed to the target 420, the triage device 140 takes at least one of

three possible courses of action: discard the packet, proxy a reply on behalf of the host 420, or forward the packet to the host 420. During the entire attack, the triage device 140 logs detailed forensics information in the attached database 300 for later examination.

EXEMPLARY PROCESSING

FIG. 5 illustrates exemplary processing of an attack detection sensor 145 consistent with the present invention. The attack detection sensor 145 passively monitors the traffic passing through the service provider 116 to the customers 135 [step 505]. The attack detection sensor 145 may analyze each packet passing through the service provider 116 to determine whether a DoS signature is present [step 510]. The attack detection sensor 145 may use any conventional DoS signature detection technique. In a smurf type of DoS attack, as described above, an attacking device causes a host device to crash by sending ping requests to a broadcast address on the host's network. The attacking device sets the return address to the victim's address, causing hundreds of response messages to be generated that eventually overload the network. In such an attack, the attack detection sensor 145 may detect the presence of the ping response messages. As part of its monitoring process, the attack detection sensor 145 may also continuously record information regarding the packets passing through the service provider 116 in an associated buffer (or database).

If the attack detection sensor 145 determines that no such signature exists in the packets passing through the service provider 116 [step 510], the attack detection sensor 145 returns to step 505 and continues to monitor the traffic. If, on the other hand, a DoS signature exists [step 510], then the attack detection sensor 145 may notify the service provider 116 and, possibly, the triage device 140 of the presence of an attack [step 515]. The attack detection sensor 145 may also

notify the service provider 116 and triage device 140 of the identity of the intended victim device (e.g., host device 420 in FIG. 4). In an alternative implementation, the service provider 116 may determine the identity of the intended victim device.

Upon notifying the service provider 116 and triage device 140 of the attack, the attack detection sensor 145 returns to step 505 and continues to monitor the traffic passing through the service provider 116. At any time during this processing, the attack detection sensor 145 may receive a request from the triage device 140 requesting a recent history of packets transmitted to the target device. In response to such a request, the attack detection sensor 145 may transmit the information recorded in its buffer to the database 300 associated with the triage device 140. This information may be later used to characterize the early or precursor phases of the attack.

FIGS. 6A and 6B illustrate an exemplary process, consistent with the present invention, that protects communication networks and devices against denial of service attacks. Processing begins when a service provider, such as service provider 116, receives notification that a DoS attack has been detected [step 605]. The service provider 116 may, for example, receive the attack detection notification from an attack detection sensor, such as attack detection sensor 145, from the target device, or from another network device.

In response to the attack notification, the service provider 116 begins to route any information received for the intended victim (i.e., host device 420) to the triage device 140 [step 610]. The service provider 116 determines whether a particular packet is intended for the host device 420 by, for example, examining target address information in the packet's header.

In response to receiving one or more packets, the triage device 140

examines each packet to determine whether the packet is part of the DoS attack [step 615]. In the example above, the triage device 140 may determine whether the packet is a ping response message.

If a packet is determined to not be part of the DoS attack [step 620], the triage device 140 may forward the packet to the host device 420 [step 625]. The triage device 140 may be configured to prioritize or filter packets to be forwarded based on a variety of characteristics, or can forward packets on a first come, first delivered basis. The triage device 140 may, however, drop packets in excess of the host device's 420 rated capacity to prevent a deluge of "good" packets from bringing down the host device 420.

If a packet is determined to be a part of the DoS attack [step 620], the triage device 140 may discard the packet and/or proxy a reply to the attacking device on behalf of the host device 420 [step 630]. By proxying a reply to the attacking device, the attacking device may be left with the impression that the DoS attack was successful. In addition, this may aid in tracking the source of the attack.

In an implementation consistent with the present invention, the triage device 140 may receive a profile from the host device 420 describing the types of packets that the host device normally receives. If such a profile has been received by the triage device 140, the triage device 140 may divert all packets not of the types normally received as likely attack material, even if of an unknown attack variety. Moreover, if the host device 420 is capable of notifying the triage device as to which IP addresses are "good," then the triage device 140 can filter good packets from attack packets, based on their IP address, even if they fall within the profile of an attack.

For each packet received during the DoS attack, the triage device 140 stores

information regarding the packet in database 300 [step 635]. As described above, this information may include the source address, target address, date, time, and other information that may facilitate later analysis of the attack.

The triage device 140 may then determine whether the DoS attack has ended [step 640] (FIG. 6B). The triage device 140 may, for example, automatically determine that the attack has ended after a predetermined period of time or after a predetermined number of "good" packets have been received without having received a "bad" packet. Alternatively, the service provider 116 or some other network device may determine that the DoS attack has ended.

If the attack has not ended, the service provider 116 continues to route packets intended for the host device to the triage device 140 [step 610] (FIG. 6A). The triage device 140 continues to process packets until the service provider 116 discontinues redirecting packets from the target to the triage device 140.

Once the DoS attack has ended [step 640], the service provider 116 may then begin to route traffic directly to the host device 420 [step 645]. Also, the triage device 140 may transfer information about the attack from its associated database 300 to a network administrator so that remedial measures may be commenced. This transfer of information may alternatively occur during the attack. The transfer may occur automatically or in response to a request from the network administrator.

CONCLUSION

Systems and methods consistent with the present invention provide a mechanism that protects communication networks and devices against denial of service attacks. Upon detection of a DoS attack, a service provider can redirect traffic away from a targeted host (or hosts) and toward a triage device, that may use a combination of packet destruction, proxying for the target, other filtering

mechanisms, and prioritized packet forwarding to protect intended targets from attack. The triage device diverts the brunt of the attack from the targets, allowing them to continue to operate during a DoS attack. Due to its modular nature, the triage device provides a flexible base for deploying new DoS attack responses as DoS attack techniques evolve. Moreover, the triage device is capable of being scaled from a single system to a multi-module, multi-homed architecture, providing cost-effective deployment for a growing target base.

The foregoing description of exemplary embodiments of the present invention provides illustration and description, but is not intended to be exhaustive or to limit the invention to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practice of the invention. For example, while a series of steps have been shown with respect to FIGS. 5, 6A, and 6B, the order of the steps may vary in other implementations consistent with the present invention.

The scope of the invention is defined by the following claims and their equivalents.

WHAT IS CLAIMED IS:

1. A system that protects against denial of service (DoS) attacks, comprising:

a service provider configured to receive a signal indicating detection of a DoS attack, receive one or more packets intended for a victim device, and transmit the one or more packets; and

a triage device configured to receive the one or more packets, determine whether each of the one or more packets is related to the DoS attack, and forward any packets that are unrelated to the DoS attack to the victim device.

2. The system of claim 1 further comprising:

a passive attack detection sensor configured to examine packets transmitted in a network for a DoS signature and transmit the signal to the service provider when a DoS signature is detected.

3. The system of claim 2 wherein the passive attack detection sensor is further configured to:

store information about the packets when the DoS signature is detected.

4. The system of claim 3 wherein the passive attack detection sensor is further configured to:

transmit the information to the triage device.

5. The system of claim 1 wherein the victim device transmits the signal to the service provider indicating detection of a DoS attack against itself.

6. The system of claim 1 wherein the triage device is further configured to:

discard any packets that are related to the DoS attack.

7. The system of claim 1 wherein the triage device is further configured to:

proxy a reply to a packet that is related to the DoS attack.

8. The system of claim 1 wherein the triage device includes a database configured to store information relating to the DoS attack.

9. The system of claim 8 wherein the triage device is further configured to:

transfer the information relating to the DoS attack to a network administrator for determining characteristics of the DoS attack.

10. The system of claim 1 wherein the triage device is further configured to:

determine an end to the DoS attack and transmit a signal indicating the end to the DoS attack to the service provider.

11. The system of claim 10 wherein the service provider is configured to:

receive the signal indicating the end to the DoS attack and transmit packets directly to the victim device in response to the signal received.

12. The system of claim 1 wherein the triage device is further configured to:

receive a normal packet profile,

determine whether each of the one or more packets matches the profile, and

discard any packets not matching the profile.

13. The system of claim 1 wherein the triage device is further configured to:

receive a list of acceptable source addresses,

determine whether a source address associated with each of the one or more packets matches an acceptable source address in the list of acceptable source addresses, and

discard any packets having a source address not matching an acceptable source address in the list.

14. A system that protects against denial of service (DoS) attacks, comprising:

means for detecting an occurrence of a DoS attack;

means for determining a target of the DoS attack;

means for intercepting at least one packet destined for the target;

means for preventing the at least one packet from reaching the target when the at least one packet is part of the DoS attack.

15. A method that protects against denial of service (DoS) attacks, comprising:

detecting an occurrence of a DoS attack;

determining a target of the DoS attack;

intercepting packets destined for the target; and

preventing packets that are related to the DoS attack from reaching the target.

16. The method of claim 15 wherein the detecting includes:

detecting a DoS signature.

17. The method of claim 15 wherein the preventing includes:

discarding a packet when the packet is part of the DoS attack.

18. The method of claim 15 wherein the preventing includes:

proxying a reply to a device that sent a packet when the packet is part of the DoS attack.

19. The method of claim 15 wherein the preventing includes:

forwarding a packet to the target when the packet is not part of the DoS attack.

20. The method of claim 15 further comprising:

storing information about a packet when the packet is part of the DoS attack.

21. The method of claim 20 wherein the information includes at least one of a source address and forensic data.

22. The method of claim 20 further comprising:

routing the information to a network administrator for performing at least one of analysis, characterization, and reporting of the DoS attack.

23. The method of claim 15 wherein the intercepting includes:

transferring packets for the target from an Internet service provider to a triage device.

24. The method of claim 15 wherein the preventing includes:

receiving a normal packet profile,

determining whether each of the packets matches the profile, and

discarding any packets not matching the profile.

25. The method of claim 15 wherein the preventing includes:

receiving a list of acceptable source addresses,

determining whether a source address of each of the packets matches an acceptable source address in the list of acceptable source addresses, and

discarding any packets having a source address not matching an acceptable source address in the list.

26. A device for protecting against denial of service (DoS) attacks, comprising:

a memory configured to store instructions; and

a processor configured to execute the instructions to receive, once a DoS attack has been detected, packets from a service provider, determine, for each packet, whether the packet is related to the DoS attack, forward the packets determined to be unrelated to the DoS attack to a target device, and at least one of discard the packets and proxy a reply to the packets determined to be related to the DoS attack.

27. The device of claim 26 wherein the processor is further configured to:

store information in the memory for each of the packets determined to be related to the DoS attack.

28. The device of claim 27 wherein the information includes at least a source address associated with the packet determined to be related to the DoS attack.

29. The device of claim 26 wherein the processor is further configured to:

receive a normal packet profile,

determine whether each of the packets matches the profile, and

discard any packets not matching the profile.

30. The device of claim 26 wherein the processor is further configured to:

receive a list of acceptable source addresses,

determine whether a source address in each of the packets matches a source address in the list of acceptable source addresses,

discard each packet having a source address not matching a source address in the list of acceptable source addresses.

31. A computer-readable medium containing instructions for controlling at least one processor to perform a method that protects against denial of service (DoS) attacks, the method comprising:

receiving, once a DoS attack has been detected, packets intended for a target device;

determining, for each of the packets, whether the packet is part of the DoS attack;

forwarding packets determined not to be part of the DoS attack to the target device; and

discarding packets determined to be part of the DoS attack.

32. The computer-readable medium of claim 31 further comprising:

proxying a reply on behalf the target device to a source device when a packet is determined to be part of the DoS attack.

33. The computer-readable medium of claim 31, wherein the determining includes:

receive a normal packet profile, and

determine whether each of the packets matches the profile.

34. The computer-readable medium of claim 31, wherein the determining includes:

receive a list of acceptable source addresses, and

determine whether a source address in each of the packets matches a source address in the list of acceptable source addresses.

35. A method that protects against denial of service (DoS) attacks, comprising:

passively recording, via by an attack detection sensor, packets transmitted in a network;

detecting an occurrence of a DoS attack;

transferring, in response to the detecting, packets for a target of the DoS attack from a service provider to a triage device;

retrieving recently recorded packets from the attack detection sensor;

determining, for each transferred packet, whether the packet is part of the DoS attack;

forwarding a packet determined not to be part of the DoS attack to the target; and

discarding or proxying a reply to a packet determined to be part of the DoS attack.

36. An attack detection sensor comprising:

a memory configured to store instructions and information relating to packets transferred in a network; and

a processor configured to execute the instructions to monitor the packets, store the information in the memory, detect a denial of service attack signature in one or more of the packets, send a signal to a service provider in response to the detecting, and transfer the information in the memory for use in determining a history of the one or more packets.

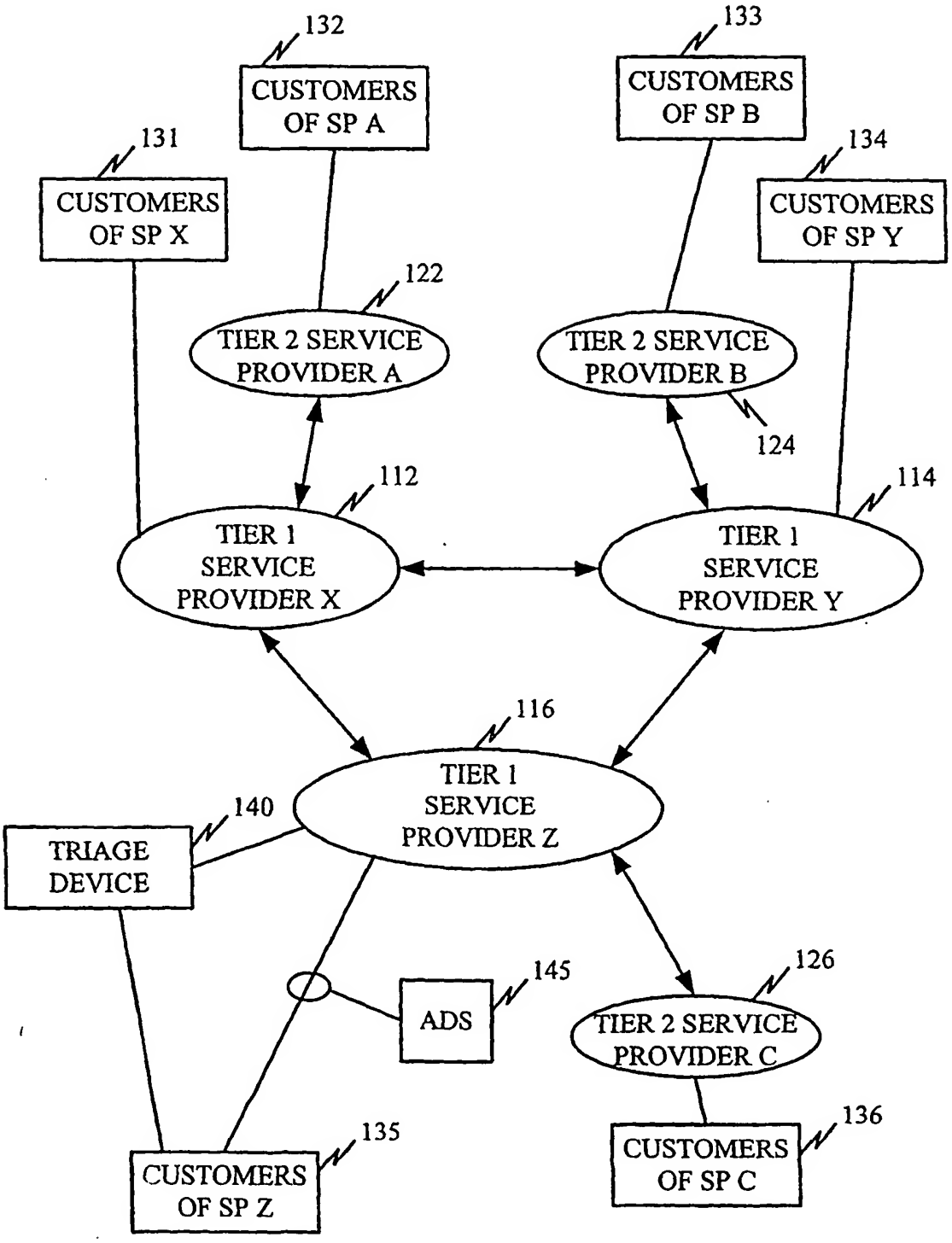

100
132
CUSTOMERS OF SP A
133
CUSTOMERS OF SP B
131
CUSTOMERS OF SP X
134
CUSTOMERS OF SP Y
122
TIER 2 SERVICE PROVIDER A
TIER 2 SERVICE PROVIDER B
124
112
114
TIER 1 SERVICE PROVIDER X
TIER 1 SERVICE PROVIDER Y
116
TIER 1 SERVICE PROVIDER Z
140
TRIAGE DEVICE
145
ADS
126
TIER 2 SERVICE PROVIDER C
135
CUSTOMERS OF SP Z
136
CUSTOMERS OF SP C

FIG. 1

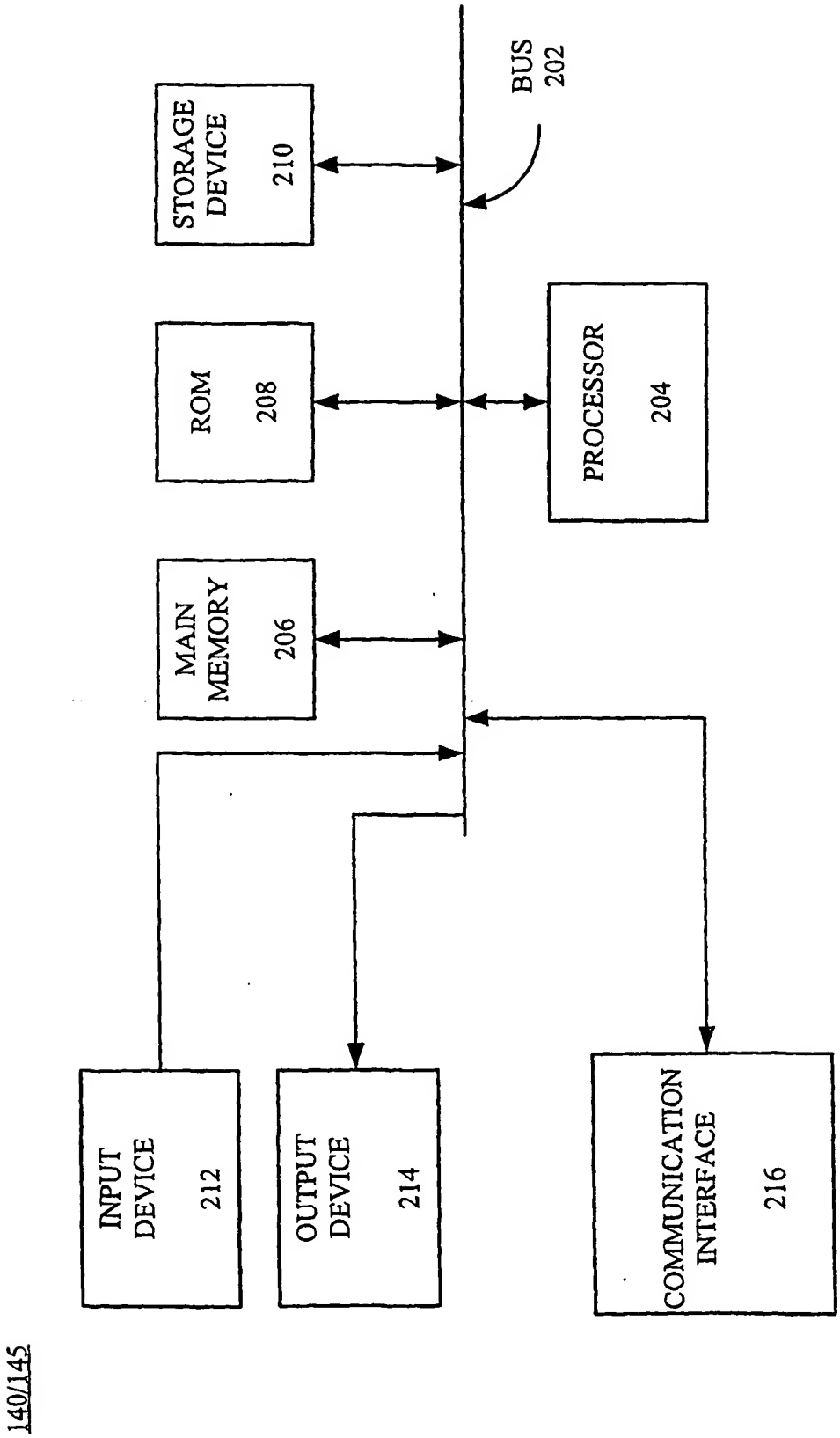

BUS
202
STORAGE DEVICE
210
ROM
208
PROCESSOR
204
MAIN MEMORY
206
INPUT DEVICE
212
OUTPUT DEVICE
214
COMMUNICATION INTERFACE
216
140/145

FIG. 2

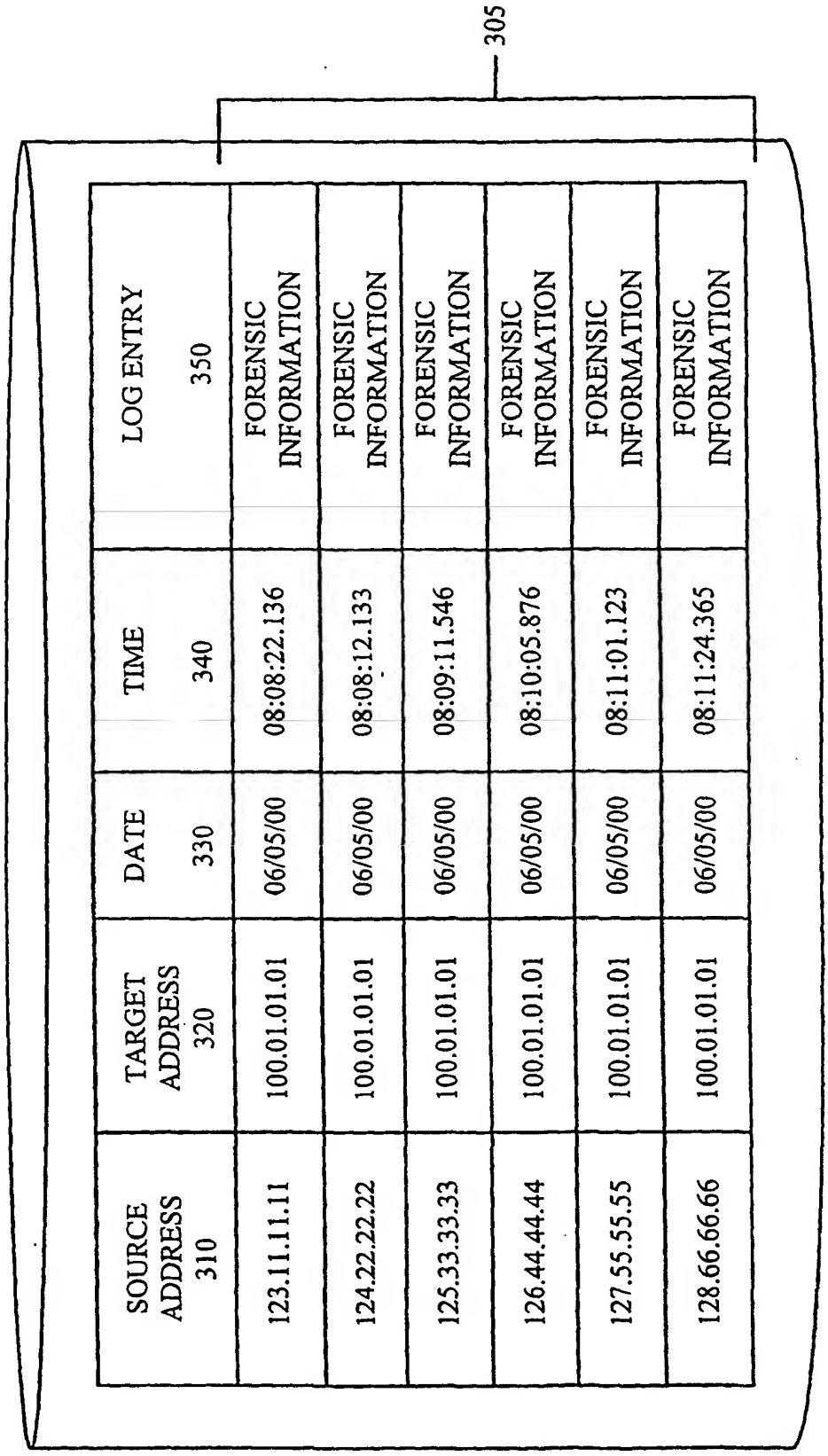

300
305
SOURCE ADDRESS 310
TARGET ADDRESS 320
DATE 330
TIME 340
LOG ENTRY 350
123.11.11.11
100.01.01.01
06/05/00
08:08:22.136
FORENSIC INFORMATION
124.22.22.22
100.01.01.01
06/05/00
08:08:12.133
FORENSIC INFORMATION
125.33.33.33
100.01.01.01
06/05/00
08:09:11.546
FORENSIC INFORMATION
126.44.44.44
100.01.01.01
06/05/00
08:10:05.876
FORENSIC INFORMATION
127.55.55.55
100.01.01.01
06/05/00
08:11:01.123
FORENSIC INFORMATION
128.66.66.66
100.01.01.01
06/05/00
08:11:24.365
FORENSIC INFORMATION

FIG. 3

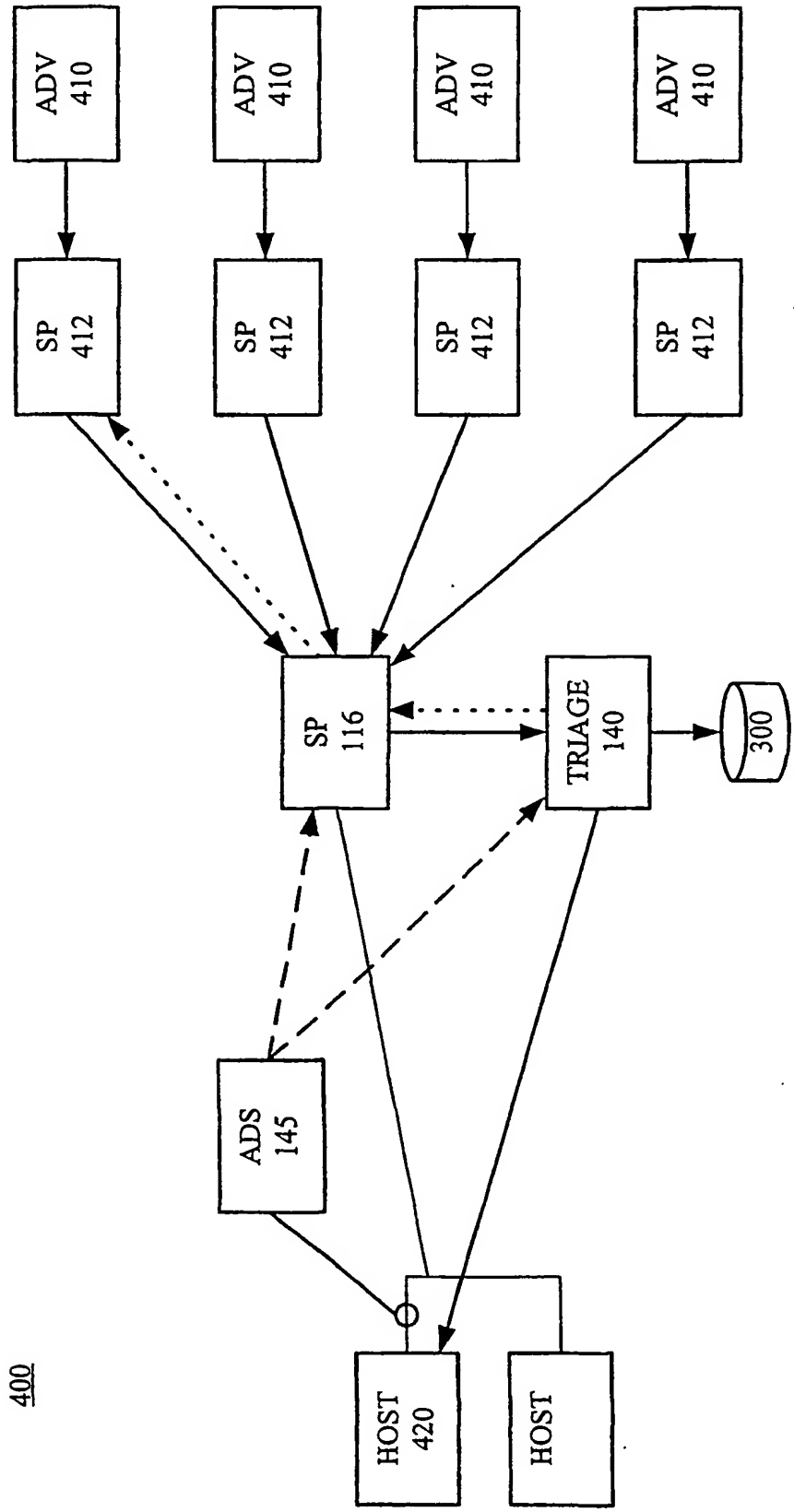

ADV 410
ADV 410
ADV 410
ADV 410
SP 412
SP 412
SP 412
SP 412
SP 116
TRIAGE 140
300
ADS 145
HOST 420
HOST
400

FIG. 4

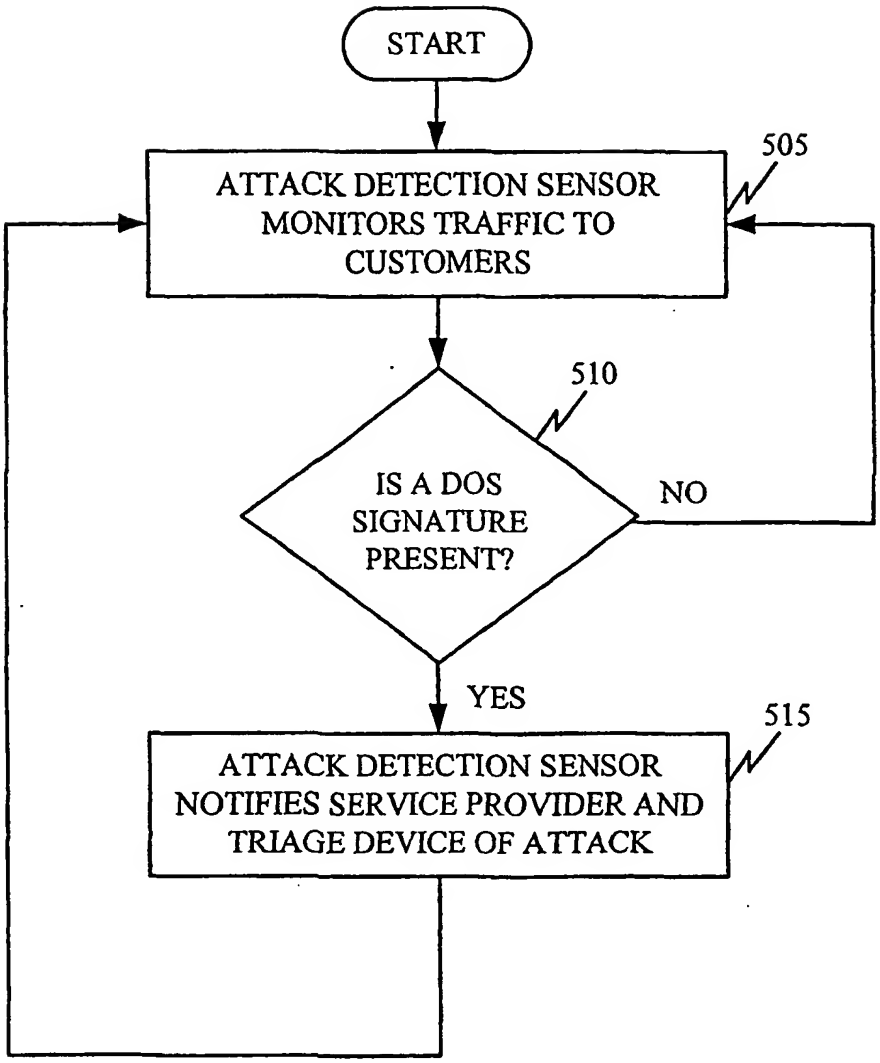

START
ATTACK DETECTION SENSOR MONITORS TRAFFIC TO CUSTOMERS
505
510
IS A DOS SIGNATURE PRESENT?
NO
YES
ATTACK DETECTION SENSOR NOTIFIES SERVICE PROVIDER AND TRIAGE DEVICE OF ATTACK
515

FIG. 5

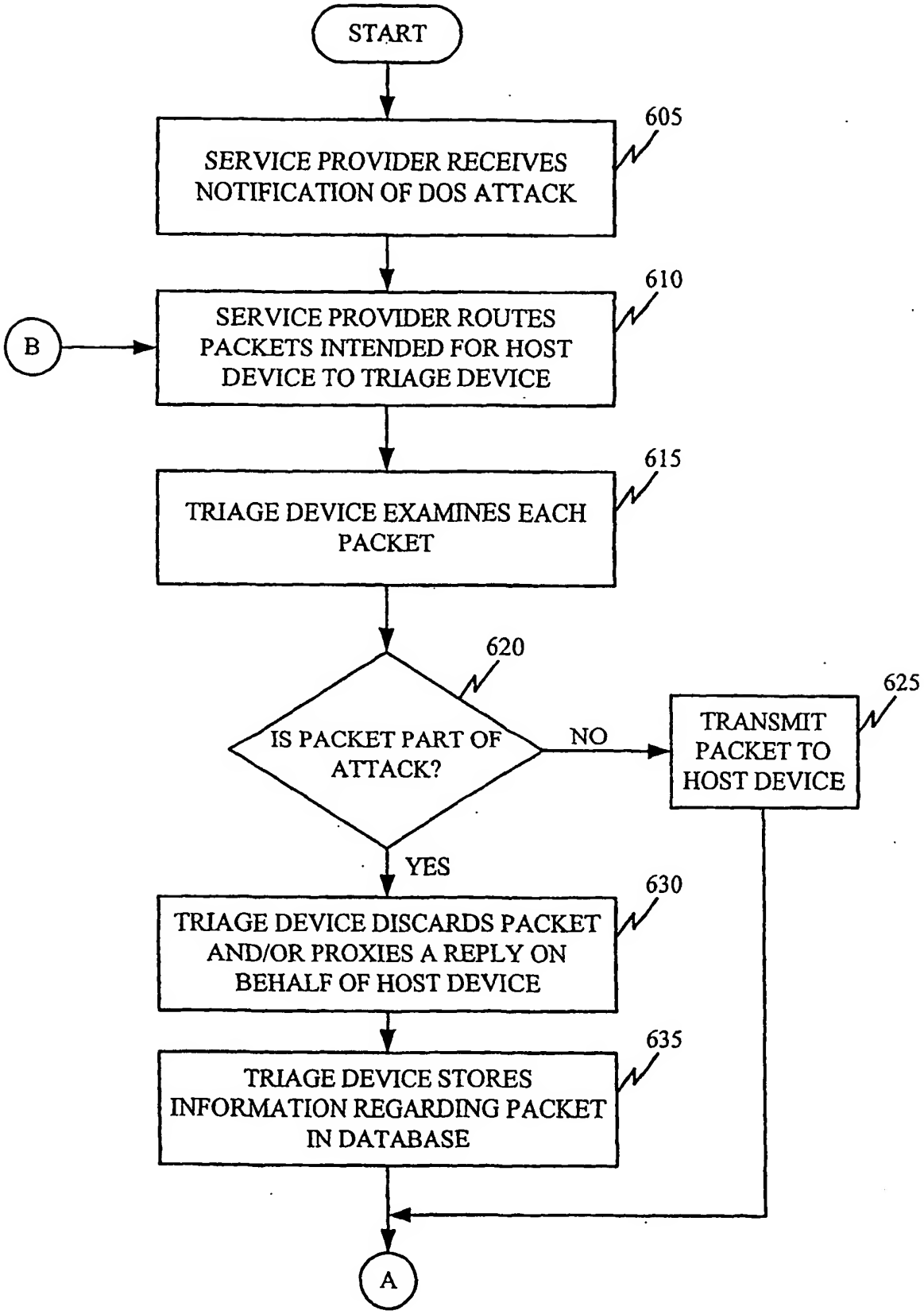

START
605
SERVICE PROVIDER RECEIVES NOTIFICATION OF DOS ATTACK
610
B
SERVICE PROVIDER ROUTES PACKETS INTENDED FOR HOST DEVICE TO TRIAGE DEVICE
615
TRIAGE DEVICE EXAMINES EACH PACKET
620
IS PACKET PART OF ATTACK?
NO
625
TRANSMIT PACKET TO HOST DEVICE
YES
630
TRIAGE DEVICE DISCARDS PACKET AND/OR PROXIES A REPLY ON BEHALF OF HOST DEVICE
635
TRIAGE DEVICE STORES INFORMATION REGARDING PACKET IN DATABASE
A

FIG. 6A

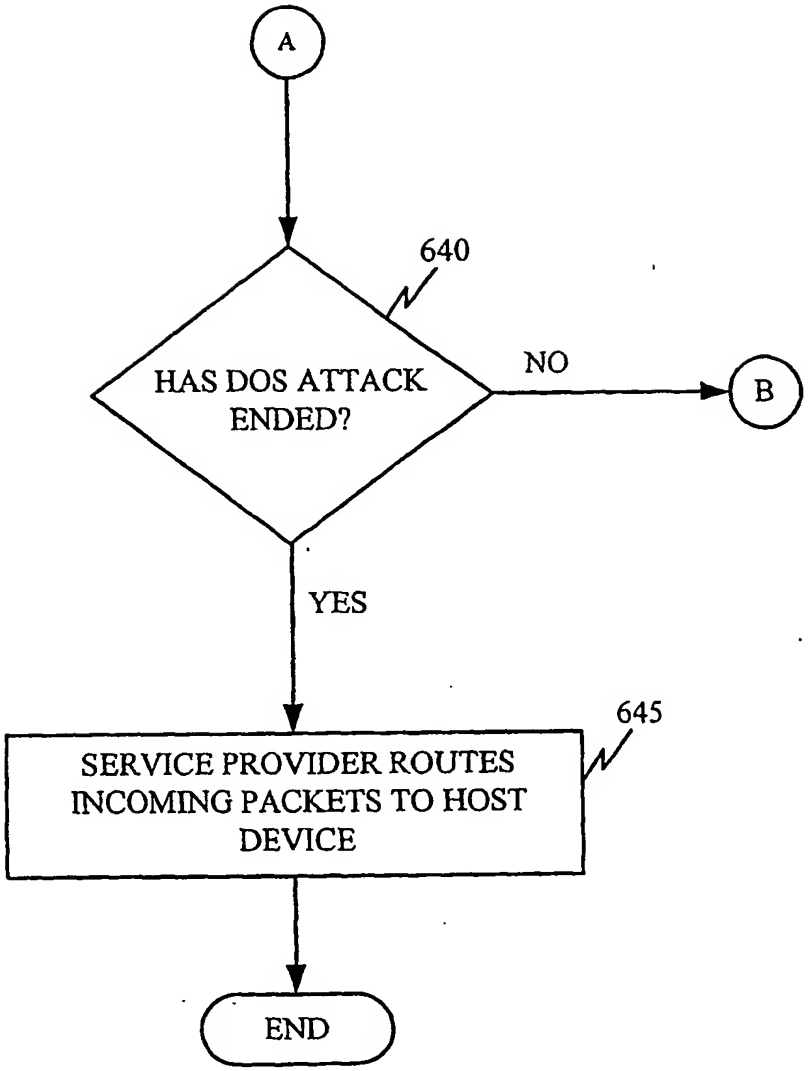

A
640
HAS DOS ATTACK ENDED?
NO
B
YES
645
SERVICE PROVIDER ROUTES INCOMING PACKETS TO HOST DEVICE
END

FIG. 6B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/29336

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00
US CL : 713/200

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/200, 153, 154; 709/224, 225, 226

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	VAZHKUDAI, S.; MAGINNIS, T., A High Performance Communication Subsystem for PODOS, Mississippi University, Mississippi. December 1999, pages 81-91, especially pages 81 (8th paragraph) and 84 (2-3rd paragraph), and especially page 86.	1-36
X,P	US 6,298,445 B1 (SHOSTACK, et al.) 02 October 2001, see COL.5, lines 20-51; COL.6, lines 36-55; COL.7, lines 37-65; COL.12, lines 14-55	1-36
A	US 6,301,668 B1 (GLEICHAUF, et al.) 09 October 2001, see COL.5, lines 39-51; COL.6, lines 37-60; COL8., lines35-57; COL.9, lines 49-54	1-36
A	SMITH, R.; BHATTACHARYA, S., Operating Firewalls Outside the LAN Perimeter, Motorola Inc., Arizona. February 1999, pages 493-498.	1-36
A	US 5,958,053 A (DENKER) 28 September 1999, see COL.6, lines 20-60; FIG.4, COL.7, lines 5-45; COL.9, lines 35-59; COL.15, lines 23-65; COL.16	1-36

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
26 January 2002 (26.01.2002)

Date of mailing of the international search report
18 APR 2002

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
Hayes Gail
for James R. Matthews

Telephone No. (703) 305-3853

Form PCT/ISA/210 (second sheet) (July 1998)